Integration of Forensic Techniques into the Threshold of Admissibility of Computer Derived Evidence: Should the Paradigm be Re-phrased?

Abu Hena Mostofa Kamal*

Abstract

During the last half of the 20th century, a remarkable shift from paper to bits has occurred. This spectacular shift combined with the ability and necessity to bring digital data to court, however, creates a critical question- "How do we prove the integrity of this new form of information known as digital evidence in the court"? This article vividly discusses the procedure to preserve the evidential integrity of computer derived documents. The article further focuses on the numerous vulnerabilities and threats that are inherent within computer generated evidence and discusses techniques to identify, retrieve, and protect valuable digital evidence for litigation and prosecution. Moreover, it deals with many issues related to the admissibility of digital evidence in court proceedings, specifically 'the Best Evidence Rule'. It further tries to determine the weight of the purported content of the computer files or digital document. In addition, this article discusses the substantial and complex tests of admissibility of "computer records" and its present status in Bangladeshi Law and determines the precise status of a printout document from a computer as primary evidence.

Keywords: Computer Generated Evidence, Computer Forensics, Digital Discovery, Computer Generated Record, Retention And Destruction Of Computer Generated Evidence, Digital Or Computer Generated Records Management, Digital Forensic Investigation, Digital Evidence.

In any event, the concept of evidence is inseparable from that of justification. When we talk of 'evidence' in an epistemological sense we are talking about justification: one thing is 'evidence' for another just in case the first tends to enhance the reasonableness or justification of the second…A strictly nonnormative concept of evidence is not our concept of evidence; it is something that we do not understand. *--Jaegwon Kim (1988)*

Introduction

Information and communication systems are now the breeding grounds for digital-evidence in audits, investigations, or litigation. The increasing number of various cyber crimes initiates the growth of collection of evidence from computers for the use of legal proceedings. Digital evidence may originate from a multitude of sources including seized computer hard-drives and backup media, real-time e-mail messages, chat-room logs, ISP records, web-pages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards,

* Assistant Professor, Faculty of Law, ASA University Bangladesh

and digital cameras. These devices are subject to computer forensic searches to identify, examine, and preserve potential digital evidence before placing it to the court for proving or rebutting any presumption. Therefore, the acquisition of reliable evidence from a computer is not always regarded as admissible in the courtroom, if accurate degree of proficiency is not used during the acquirement. This is why, increasingly, Computer Forensics Experts are being ordered by the court to preserve, retrieve, and hand-over relevant digital records (e-records).[i] For example, in a survey of 1,100 U.S. companies conducted by the American Management Association and the e-Policy Institute, 14% of respondents said they were ordered by a court or regulator to produce employee e-mail in 2002, which was up from 9% in 2001.[ii] Garry Mathiason, partner of a law firm which defends major corporations in employment cases, reported that almost every case his firm handle include an e-mail component.[iii] In 2000, email was considered as the most common type of digital evidence or computer generated evidence. In legal actions where evidence-mail or other computer generated evidence is used, it is as powerful as DNA evidence, and as hard to deny or refute.[iv]

As I said earlier, over the last few years, the courts were showing its leniency in admitting evidence derived from the hard-disks installed within computers, the removable floppy disks, CDs and DVD's used for temporary storage and the tapes and optical disks used for back-up or archive.[v] But the vast majority of computer-derived exhibits offered in legal proceedings consist of relatively normal printout documents which happen to have been produced by a computer, and which need further affirmation regarding its source.

As pointed out above, the courts are admitting printout of a data or file hosted by a computer, and in absence of any ambiguity arising from its acquisition, they are very much enthusiastic in admitting it as evidence if authenticity is guaranteed. But in many circumstances, the source of such printout straight from the computer which generated it, does not exist or is not immediately available. Therefore in absence of the source, the printout loses its evidential integrity and often is excluded from trial process.

Sometimes, a source of a printout (data or file) may only be obtainable with the consent of the computer owner or by formal discovery or disclosure and seizure. But often a computer may not contain the precise files required for proofing the authenticity of a print-out. [vi] It may be possible to secure a source of a printout (data or file) by seizure under warrant or order, "but files and file contents may be altered between the time at which it is first decided that a file is worthwhile potential evidence and the point at which a warrant or order can be executed."[vii]

In this article I am going to discuss the following facts that have profound link with the process of acquisition of digital evidence:

1) How can it be shown that the file acquired is what was on the computer? Can a printout be sourced back to its origin? What status does a printout receive if its origin (data) is not presented in the court due to unavailability? What status does a printout receive if its origin (data) is not presented in the court, though it is available?
2) What do we need to do to show that the process of acquisition is not free from error because it is relatively easy to corrupt data stored on a hard drive?

3) How do we preserve the file once it has been acquired and how are we able to show that any subsequent copying or retention or acquisition process has not introduced contamination as most digital information is easily changed, and once changed it is usually impossible to detect that a change has taken place?

Apart from these questions, I am going to emphasis on the real life situations, where courts need to consider the weight of the purported content of the files, and to know how these records were handled by the computer which has produced them and what inferences may reasonably be drawn therefrom. In addition, I would like to discuss the substantial and complex tests of admissibility of "computer records" and its present status in Bangladeshi Law.[viii]

Definition of Computer Derived Evidence or Computer Generated Evidence

Digital evidence or computer derived evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. In simple words, computer derived evidence is data from computer systems that is used as evidence in legal proceedings. [ix] More specifically, computer evidence is data, harvested from a computer hard drive and utilized in the process of a crime investigation and judiciary. It is information of probative value that is stored or transmitted in a binary form.[x] This includes not only computers in the traditional sense but also digital audio and video. Moreover, it includes all facets of crime where evidence may be found in a digital or binary form. Therefore, digital evidence can be defined as any information of probative value that is either stored or transmitted in a digital form. It includes files stored in computer hard drive, digital video, digital audio, network packets transmitted over local area network, etc. Depending on the facts that the digital evidence is supposed to prove, it can fall into different classes of evidence. [xi]

1. Digital images or software presented in court to prove the fact of possession are real evidence.
2. E-mail messages presented as proof of their content are documentary evidence.
3. Log files, file time stamps and all sorts of system information used to reconstruct sequence of events are circumstantial evidence.
4. Digital documents notarised using digital signature may fall into testimony category.[xii]

Eoghan Casey[xiii] defines digital evidence as "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi." International Organization of Computer Evidence (IOCE) proposed another definition of Computer derived evidence. According to them "Computer derived evidence is information stored or transmitted in binary form that may be relied upon court."[xiv] It is pertinent to note that the term digital evidence and electronic evidence are sometimes used interchangeably. However, an effort should be made to distinguish between electronic devices such as mobile phone and digital data that they contain.

C. Miller provides a useful broad explanation that can be used for explaining the judicial process in which computer generated evidence or digital evidence receives admissibility. He sayes,

"Evidence is information used to decide whether disputed propositions are true. A court cannot normally obtain evidence directly (first hand). A source is relied on, such as a document or human witness. The reliability of the information is assessed directly by testing the reliability of the source." [xv] He further notes, "If witnesses are used, they are cross-examined; if documents are used, a human witness is often asked to verify that a document is authentic and to give oral testimony about its content." [xvi] The following are Miller's general tests for the reliability of a computer derived Exhibit[xvii]:

(i) Computer Derived Evidence must be Authentic: The word authentic means "having a claimed and verifiable origin or authorship; [xviii] not counterfeit or copied or having the origin supported by unquestionable evidence;[xix] or conforming to fact and therefore worthy of trust, reliance." [xx] The word authentic further denotes:

1. to make authentic or valid
2. to establish the truth of; verify
3. to prove to be genuine or as represented
4. It is specifically linked to the circumstances and persons alleged. [xxi]

According to Reed[xxii], "authentication means satisfying the court that:

(a) the contents of the record have remained unchanged,

(b) that the information in the record does in fact originate from its purported source, whether human or machine, and

(c) that extraneous information such as the apparent date of the record is accurate.

(d) for the admissibility of paper records or printout, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available or via technological features in the system or the record." [xxiii]

Once evidence is found to be relevant, it must be authenticated. It means there must be a guarantee of trustworthiness attached to the evidence. [xxiv] Authentication standards are meant 'to ensure that the evidence is what it purports to be, and how rigorous a foundation is needed to make this finding depends on the existence of something that can be tested in order to prove a relationship between the evidence and an individual and control against the perpetration of fraud.'[xxv] Apart from this another evidentiary lynchpin is attached to computer derived evidence which is that "computer derived evidence must be original". This rule is known as the 'Best Evidence Rule'. As per American law the 'original' of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.[xxvi] A similar approach was discovered in Ohio v. Morris (2005).[xxvii] In this case the government's forensic analyst copied the hard drive of the Defendant's computer and returned it to the police department that seized it. However, prior to returning the computer, the analyst erased all the data on the drive. The evidence in question was actually presented at trial in the form of a copy of the hard drive. The Defendant argued that his due process rights were violated because he could not examine the

original hard drive to determine whether it contained exculpatory evidence. The appellate court held that testimony about the imaging techniques of the software used to create a copy of the original drive was sufficient to show that the duplicate was admissible as it ensured authenticity. This case suggests that exact replication of the original digital evidence derived from a computer carries the same value equivalent to the original.

To determine authenticity, the Court suggested five criteria in Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993).[xxviii]These are as follows:

1. Whether the information is derived by the scientific method,
2. Whether the information has been subjected to peer review or publication,
3. Whether the relevant scientific community 'generally accepts' the information,
4. Consideration of the actual or potential rate of error of the scientific technique, and
5. Whether standards for controlling the technique's operation exist.

These five criteria are very crucial to determine authenticity of digital evidence. Therefore, almost all digital evidences generated from computer are subject to this rule. Furthermore, the International Organization on Computer Evidence (IOCE) provided the following guidelines that can also be used for ensuring authenticity of digital evidence:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his/her possession.
6. Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.[xxix]

As I mentioned before, a computer generated data is not admissible until it has been authenticated. Authentication, in broad terms, demands:

(a) Proof of provenance--that the output is indeed the output from the devices from which it purports to arise; and

(b) Proof of reliability--that the computing devices in fact do and, on the particular occasion, did what they are supposed to do.

Therefore, an authentic value of a computer derived evidence is only recognized by the court when it successfully satisfies the mentioned criterion along with others.

Further the authentication of an electronic documents or digital data is not inherently more anonymous than a typewritten document. Indication of authenticity (relating to the identity of the creator of the document) such as signatures may have technological equivalents, such as digital signatures. Similarly, "the date on which a document is created or amended is not inherently more difficult to prove than any other form of document: indeed, sometimes it may be easier to discover the date on which an electronic document was created than the date on which a hand-written or typewritten document was created. Thus, for example, the sender of an electronic

message should be in no worse a position to offer oral evidence to authenticate that message than the sender of a paper message." [xxx]
Long-standing American authority suggests that the authenticity of computer documents may be established by the evidence of a person responsible for the custody and control of the records.[xxxi] As far as I know, more than a few provisions in the Evidence Act 1872, which require a specific change, are to be made to accommodate any difficulties in the authentication of computer documents. If the future law permits the presentation or retention of information in its original form, the information may be retained in electronic or digital form within the ambit of the term 'document'. [xxxii] However for this to apply there must be a reliable assurance as to the integrity of the information from the time first generated in its original form. Integrity will be a matter of evidence to be adduced before the court. This may involve a Forensic Expert to give evidence indicating that the particular computer systems involved were performing normally. Sadly, no extensive indication is given in the prevailing Act in relation to the standard of integrity of digital evidence. The courts therefore will have to examine the issue on a case by case basis and use vast discretionary power in interpreting statues that have no connection with digital arena.

(ii) Computer Derived Evidence must be Accurate: In ordinary sense, accurate means free from mistakes or errors; or precisely free from any reasonable doubt about the quality of procedures used to collect the evidence, or analyses of the evidence. Where exhibits contain statements such as an email, data, file or other document, the accuracy of the exhibits must encompass accuracy of content; and that normally requires the document's originator to make a witness statement and be available for cross- examination.[xxxiii]

In Marac Financial Services Limited v Stewart [1993][xxxiv], it was suggested that, once a contract had been entered into, evidence produced by a computer without human input may only be excluded if the party opposing the admission of evidence can prove that the technology which created it, had been recently invented or that its reliability had not been established by use over a period of time. This test creates a presumption that computer generated records are reliable in the absence of evidence to the contrary.

However, in Ministry of Agriculture and Fisheries v Thomas [1994][xxxv] , it was held that, in addressing the question whether technology was recently invented or reliable, it was not the restricted community of users to be taken into account but, rather, the "community at large". In so holding, the judge took the view that the reference in the Court of Appeal, by Richardson J (in Holt v Auckland City Council), to "a matter of common knowledge" could not include, in the community, only those who might be expected to come across the system concerned in the course of their careers.[xxxvi]

As computer generated information or data is a manifestation of the intent of that computer's owner or user [xxxvii]and as such would be admissible in most cases[xxxviii] if test of accuracy is satisfied along with others.

(iii) Computer Derived Evidence must be Complete: It means the exhibit must manifest within its own terms a complete story of a particular set of circumstances or events. A number of writers

use the terms "reliable" and "authentic" almost interchangeably and the definitions given above are the more useful for being more restricted.[xxxix]
It should be noted that digital evidence is not very different from other forms of evidence from the legal point of view. Like any other form of evidence, it has to be relevant to the dispute, and it has to pass admissibility test to demonstrate its evidential integrity. Furthermore, advanced analysis of digital evidence, such as event reconstruction, often requires specialist knowledge and, therefore, falls into the category of expert evidence. As expert evidence, it may have to pass "Daubert criteria" or similar admissibility test as per the rules of locality which verifies that its analysis methodology is scientifically sound and valid.

Vulnerability of Computer Data

The law of evidence should not be subtle and difficult to understand. And fine distinctions should only be tolerated if both unavoidable and . . . easy to make. (Re M and R (Minors) [1996] 4 All ER 239 (CA), 254)

The term vulnerability means a weakness which allows a data or digital record or electronic document to reduce its authenticity and accuracy. Vulnerability is the intersection of three elements:

(a) digital or electronic record or document's susceptibility or flaw,
(b) digital data or electronic record or document's procurement was improper to guarantee the authenticity, and
(c) digital data or electronic record or document's are not handled by technically sound person who inadvertently exposes the data to vulnerability and makes it inadmissible evidence.

To be admissible, electronic or digital evidence must be copied or procured or acquired or retained with the help of at least one applicable tool or technique that can guarantee authenticity and make the data weakness free. The only way to reduce the chance of vulnerability is to enhance constant vigilance in procurement, including careful system maintenance, best practices in deployment and auditing.[xl] Here, I shall discuss the vulnerabilities or flaws which set computer-derived evidence apart.

(i) Computer data can change moment by "moment within a computer and along a transmission line. Many forms of conventional evidence are claimed to be a 'snapshot' of a particular sequence of circumstances, but the problems are particularly acute with computers"[xli] as its contents are more vulnerable to intentional and unintentional alterations. For example, in 1990, the AT&T network virtually collapsed because of software error that prevented millions of people from making long distance calls for a period of nine hours. In 1985 faulty software caused the Bank of New York to be overdrawn with the Federal Reserve by 23 billion dollars and it lost 5 million dollars in interest on overnight loans. A number of Space Shuttle missions have been delayed because of improper interaction between hardware and software. In 1992 the London Ambulance Service, the

largest in the world, was unable to answer emergency requests owing to problems with its Computer Aided Dispatch System.

(ii) Computer data are subject to easily alteration and it can be done without leaving any trace that such alteration has taken place. Alterations in hand-written and typed documents are usually self-evident and visible to naked eye. Real world documents like log book and account books are designed to detect any false entry to enhance/cntrol accountability and authenticity. Though there exist plenty of examples of forgery which make typed and hand-written originals less trustworthy, yet to some extent computer-based documents are more forgery prone than real world documents. Computer-based documents can be forged easily. It is also free from easy detection.

(iii) Digital data stored on magnetic and optical media or other storage like hard disk can be damaged by a variety of causes. Dampness, strong magnetic fields, ultraviolet radiation, and incompetent use of storage devices and recklessness in using examination tools are some of the possibilities. Further digital information is highly sensitive to minor changes. [xlii]A single bit change may cause dramatic change in its interpretation. It is true that minor changes are very hard to detect in a large quantity of digital information, particularly if the damaged information has valid interpretation. To minimise the impact of this problem, "typical storage devices use 'check summing' and similar means allowing them to reasonably reliably detect accidental information damage."[xliii]

(iv) Computer derived materials are also vulnerable to contamination. During the time of procurement, computer generated evidence can be easily altered as a result of flawed process of collection. To some extent the problems with some computer-derived materials are intense than biological materials. For example, the very act of opening an application or file, even if there is no intention to alter anything, often creates invisible changes.[xliv]

There are many forms of forensic techniques which can be employed to reduce the risk of contamination. Only a good forensic expert with an apt knowledge in computer can assure the required procedure in collecting evidence from a computer. It is pertinent to note that admissible computer generated evidence must assure the following elements:

1. Chain of custody / continuity of evidence;
2. Transparent forensic procedures;
3. Accuracy of process;
4. Accuracy of content;
5. Explanations.

Unfortunately, in the Information & Communication Technology Act 2006 or Evidence Act-1879, I could not find any provision which provides sufficient guideline for the procurement or acquisition or retention of computer generated evidence or instruction for fulfilling the above requirements. This is indeed very frustrating. If the chances of contamination are higher than the authenticity in the procurement and examination stage, then in due process the evidence will lose its admissibility. With the lack of sufficient guidelines and inadmissible evidence generated from

a computer system, how could it be possible to provide justice to the aggrieved party? It's a rhetorical question, which can only be answered by the concerned persons who are involved in law making process and judiciary.

As I pointed out earlier that ICT Act failed to provide robust guideline for the acquisition & retention of computer generated evidence. Here I would like to refer to Section 9 of the ICT Act, 2006[xlv] in favor of my arguments. Section 9 of the ICT Act, 2006 provides that:

(1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:

(a) The information contained therein remains accessible so as be usable for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) A person may satisfy the requirements referred to in subsection (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

(3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records.

As mentioned in section 9 (1) (b), originality/ authenticity must be preserved during retention and acquisition of computer documents (The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received). But this provision does not prescribe any procedure for retention of any digital document in its original form. As we know, "computer evidence is the large number of possible and potentially accurate representations of original computer data that can exist. What is seized may be a computer disk which in turn contains large numbers of directories of files of various kinds, while what is put immediately before the Court may be any of a number of purportedly accurate printouts or screen dumps. The large variety of possible representations of original material makes difficult the evolution of 'standards'. …..and the possibilities for inaccurate representation are very much greater. Nearly always, computer-derived exhibits require that the court make a chain of inference before reaching a conclusion."[xlvi] If the existing law requires data to be retained in its original form, this requirement is only fulfilled if the information is retained in electronic form subject to the assurances regarding its integrity from the date of its creation to the date in question so long as

the information remains complete and unaltered.[xlvii] Similarly, there may be a requirement to produce evidence of an expert witness in relation to the digital evidence.

Further, in the ICT Act, the exact qualification of a forensic expert is not penned yet. In Bangladesh, we do not have a national accreditation program for expert witnesses in computer forensics which would definitely assist the courts in testing the qualifications of expert witnesses. In absence of provisions regarding the qualification of an expert in the Act, courts are having more discretionary power to chose computer forensic experts, which often is subject to abuse. As I said earlier that computer forensic expert plays a vital role in judicial process, and selection of experts must not be done in haste. Sometime, a qualified expert may shed light to a dark arena and trace new evidence which in long run change the verdict. For example, in the case of Peach v Bird (2006)[xlviii], the defendant had been acquitted of charges of possessing child pornographic images. An appeal was lodged. Although no images of child pornography were able to be recovered from the hard drive, the forensic examiner, using "En-Case software" found various incriminating file names as well as evidence that the hard drive had been erased and overwritten in an attempt to remove evidence. The forensic examiner reported that:

[T]he hard drive of the computer contained a word document named 'untitled document.wps' ('the untitled word document'). The document was found in the computer folder, C:\\My Documents. The word document contained a number of links to or addresses of websites, including the link, 'http:// mx.photos.yahoo.com/pishanito2002' (the pishanito website). The hard drive of the computer also contained a directory of 70 images and one temporary storage file of a word document that had been stored in the C:\\My Documents\\My Pictures folder of the computer. The 70 images and the one word document contained in the directory had been overwritten or erased with the use of eraser programs on the computer. This meant that the 71 files could no longer be recovered. All that could be seen was the name of each file that had been saved to the C:\\My Documents\\My Pictures folder of the hard drive; the date that each file was created and the date that each file was overwritten or erased. Unlike a file which has been merely deleted, a file which has been overwritten or erased cannot be recovered. The erasing programs on the computer had been run on the files/images rather than the whole of the folder including the directory of file names of the 70 images and one word document. One of the files of the 70 erased images in the directory was named 8087053lg0.jpg. A jpg file is an image or picture file as opposed to a text file. The file named 8087053lg0.jpg was created on 17 March 2003 and overwritten or erased on 18 March 2003.

Based on this evidence, the acquittal was set aside and a retrial ordered. On 28 August 2006, an appeal was also dismissed.[xlix]

Further, in the ICT Act, there are provisions for confiscating any computer system if it is linked with a cyber crime for acquiring evidence. But I did not find any provision relating to 'Evidence Preservation Order' in the Act. In many countries, court has the jurisdiction to issue an Evidence Preservation Order for acquiring an individual's digital records or a company's digital records which include active data, data archives, metadata, network logs, cookies, web usage logs, email, and IM. To ensure computer generated evidence, preservation, backup or maintenance operations

are usually requested. A court may specifically order an individual or a company to freeze their backup tapes, data and to create and retain new backup tapes on an ongoing basis after the litigation is under way. An order to freeze backup tapes can generate significant costs if backup systems[l] and schedules need to be reconfigured. But court not even bothers to impose 'Evidence Preservation Order', if it is needed most for providing justice. Those costs are often in the millions of dollars. For example, the cost of the effort to reconstruct, retrieve and analyse e-mail related to the Monica Lewinsky case was $11.7 million.[li]

The Federal Court of Australia, in the case of Kabushiki Kaisha Sony Computer Entertainment v Stevens [2002][lii], said that "visualising the actual size of digital data as it has been noted that in a number of court case trials, judges, prosecutors and unassisted defence lawyers have asked for all data on a computer exhibit to be printed out. In many technology-enabled cases, a printout of all data produced as a result of an examination will be infeasible. For example, the amount of information gathered during the investigation in Operation Firewall by the United States Secret Services is estimated to be approximately two terabytes – the equivalent of an average university's academic library (USSS 2004). Moreover, hardcopy printout of an electronic document does not necessarily include all the information stored in the computer or electronic exhibit (e.g. data held in memory) (see Armstrong v Executive Office of the President 1 F 3d 1274 (DC Cir 1993))."

In Digicel (St Lucia) Ltd. & Others v. Cable & Wireless Plc & Others (2008)[liii], the court considered an application by the claimant for restoration of back-up tapes and for additional search terms against the Defendant. The Defendant had already conducted an extensive search of over 1 million documents at a cost of over £2 million, and claimed that the further searches would be costly and disproportionate.

In deciding whether this was a reasonable search, Mr. Justice Morgan did not use as a yardstick the more detailed search conducted by the Claimant, although he said that if the Claimant had done very much less than the Defendant, he might have questioned the application for disclosure. The Judge held that the Defendant's solicitors' failure to comply with this direction exposed the Defendant to the risk that the Court may order the search to be done for the second time. This failure also led the Judge to order that the parties should first meet and discuss how the back-up tapes should be restored, and he then ordered the Defendant to restore the tapes. He also ordered the Defendant to conduct a further search for electronic documents using some additional search words. Before making this order the Judge considered, in relation to each additional word in the Claimant's application, the proportionality of a further search being carried out and the likelihood of locating further relevant documents by that search.
So the big question arise "what to do in order to secure the 'original form' of evidence generated by computer system?" There are six methods which are used everywhere to confirm the accuracy of an evidence generated by computer. These are discussed bellow briefly:

(a) **Computer's Correct Working Test:** It must be shown to the court that the computer was behaving "correctly" or "normally" at the time the document was produced. This requirement may be related to tests of admissibility. It is necessary to show a court that the output of the computer can be relied on. Therefore, the accuracy of the data input process along with the reliability of the functionality of the computer hardware and

software must be ensured in supporting that printout was not screen dump rather authentic documentation of a file.

(b) **Provenance of Computer Source Test:** The Oxford English Dictionary defines provenance as: (i) the fact of coming from some particular source or quarter; origin, derivation; and (ii) the history or pedigree of a work of art, manuscript, rare book, etc.; concretely, a record of the ultimate derivation and passage of an item through its various owners. Hence, we can regard provenance as the derivation from a particular source to a specific state of an item. Similarly, Provenance of Computer Source Test refers (PCST) to the documented history of a datum i.e. it has been obtained from a specific computer and nowhere else.

(c) **Content/Party Authentication Test:** This process links the data from the computer to the accused or the party and the events that are the subject of legal proceedings. [liv] Given the volatility of computer files, "acquisition also usually needs to be linked to a specific day and time. This level of authentication cannot be done within a purely technological/computer context but will require other forms of evidence such as witness statements, exhibits indicating ownership of or access to the computer or data media, or the possibility of inference from the nature of the content of the files."[lv]

(d) **Acquisition Process Test:** This test gives a full and realistic explanation of the processes by which the file is acquired from the computer to show that the result is accurate, free from contamination and complete.

(e) **Continuity of Evidence/Chain of Custody Test:** This test explains what has subsequently happened to the material retrieved. As we know, the strict evidentiary requirements for criminal prosecutions suggests that there must be a demonstrable chain of custody in relation to any computer generated evidence collected, so that no reasonable doubt can be raised in relation to the authenticity and integrity of the data presented to the court. To establish a chain of custody, the trained computer forensic experts should ideally:

1. create an evidence copy of an electronic record. Such copies can be created by various means including reproducing the electronic record as a printed document or copying the electronic record to storage media (e.g. backup tape).
2. maintain a custody log of the evidence copy, recording details such as who accessed the evidence, when the evidence was accessed and returned (if evidence was removed) and why the evidence was accessed.

In particular, "authentication is needed that the contents of a computer have not been created, deleted or modified during the time of search, seizure and subsequent analysis. In this regard, it is important that the analysis be undertaken by properly trained and skilled computer forensic analysts."[lvi] The chain of custody is explained through a diagram bellow:

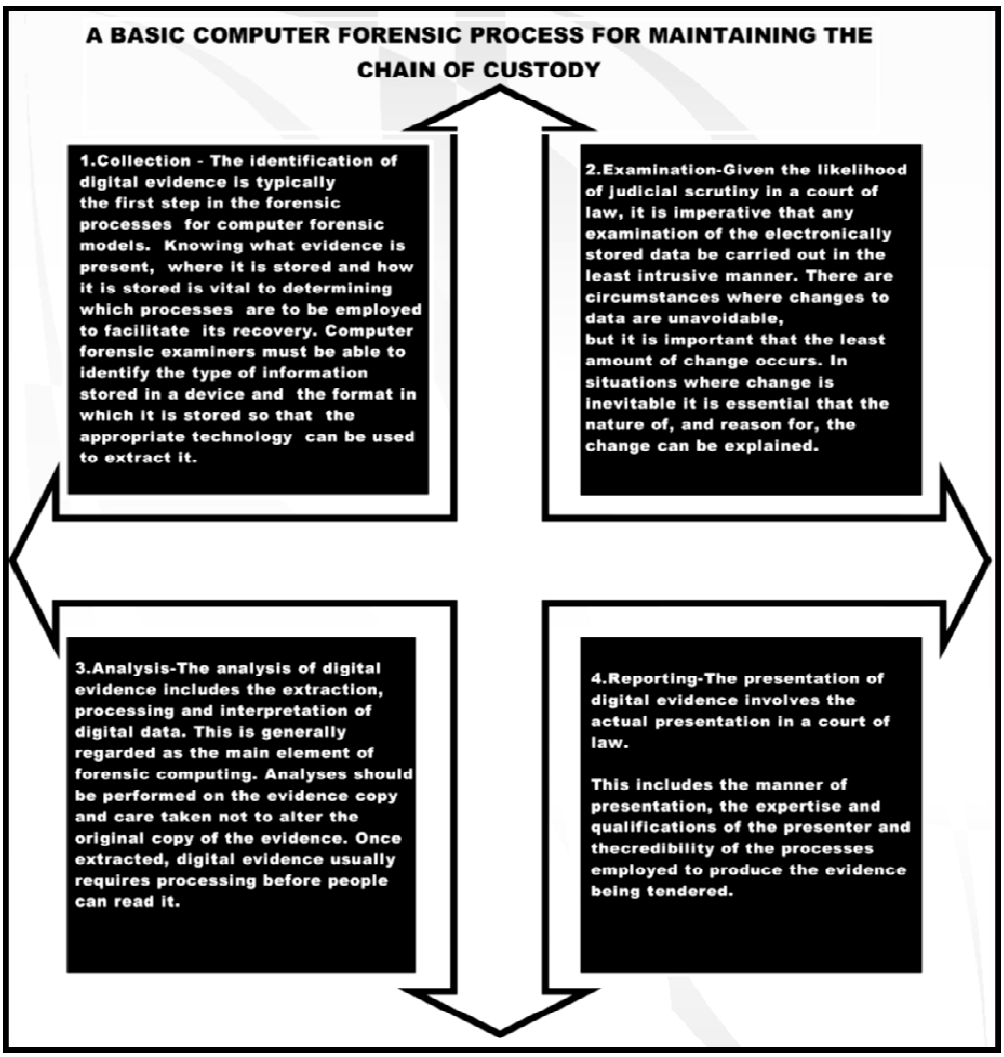

Diagram-1: Chain of Custody

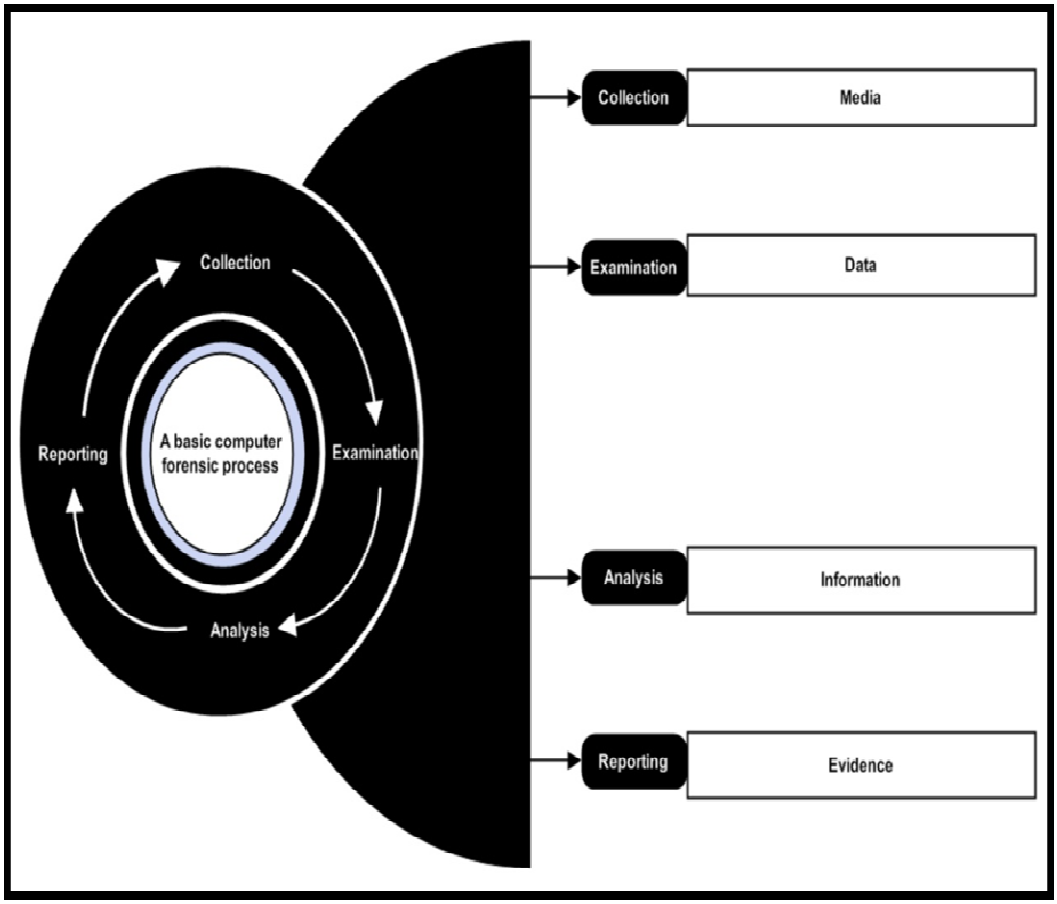

Diagram-2: Stages of Chain of Custody

(f) Quality of Forensic Presentation Test: Once the data is obtained by investigators, a subsequent processing, such as retrieval from archive formats or examination via an application program should be cautiously maintained. Special analytic tools should be used for these purposes. If files have to be decrypted, it should be done with care by maintaining log book and using proper tools. If the printout is offered as evidence, it must be shown – "how was the print-out obtained? How accurate and objective were all these methods--and how far can they be said to be generally accepted?"[lvii]

To some degree these questions must be answered by the digital forensic experts. Further, admission would be subject only to evidence of provenance and authenticity.

Apart from these, there are several methods which may be useful in proving the authenticity of digital evidence. The table below illustrates the method, advantages and disadvantages of each.

Method	*Description*	*Common Types*	*Advantages*	*Disadvantages*
Checksum	A method of checking for errors in digital data. Typically a 16- or 32-bit polynomial is applied to each byte of digital data that you are trying to protect. The result is a small integer value that is 16 or 32 bits in length and represents the concatenation of the data. This integer value must be saved and secured. At any point in the future the same polynomial can be applied to the data and then compared with the original result. If the results match some level of integrity exists.[lviii]	CRC 16 CRC 32	1. Easy to compute 2.Fast 3.Small data storage 4. Useful for detecting random errors	1.Low assurance Against malicious attack 2. Simple to create new data with matching checksum 3.Must maintain secure storage of checksum values 4. Does not bind identity with the data 5. Does not bind time with the data
One-way hash algorithm (MD2, MD4, MD5, SHA	A method for protecting digital data against unauthorized change. The method produces a fixed length large integer value (ranging from 80 – 240 bits) representing the digital data. The method is said to have one-wayness because it has two unique characteristics. First given the hash value it is difficult to construct new data resulting in the same hash. Second given the original data it is difficult to find other data matching the same hash value. [lix]	SHA-1 MD5 MD4 MD2	1. Easy to compute 2. Can detect both random errors and malicious alterations	1. Must maintain secure storage of hash values 2. Does not bind identity with the data 3.Does not bind time with the data
Digital Signature	A secure method of binding the identity of the signer with digital data integrity methods such as one-way hash values. These methods use a public key crypto-system where the signer uses a secret key to generate a digital signature. Anyone can then validate the signature generated by using the published public key certificate of the signer. The signature produces a large integer number (512 – 4096 bits)[lx]	RSA DSA PGP	1. Binds identity to the integrity operation 2. Prevents unauthorized regeneration of signature unless private key is compromised	1. Slow 2. Must protect the private key 3. Does not bind time with the data 4. If keys are Compromised or certificate expires digital signature can be invalidated

Source: Chet Hosmer(2002), Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1.

Moreover, in 1999, a Scientific Working Group on Digital Evidence (SWGDE) drafted Definitions, Standards and Principles for Acquisition of Digital Evidence. These guidelines are as follows:

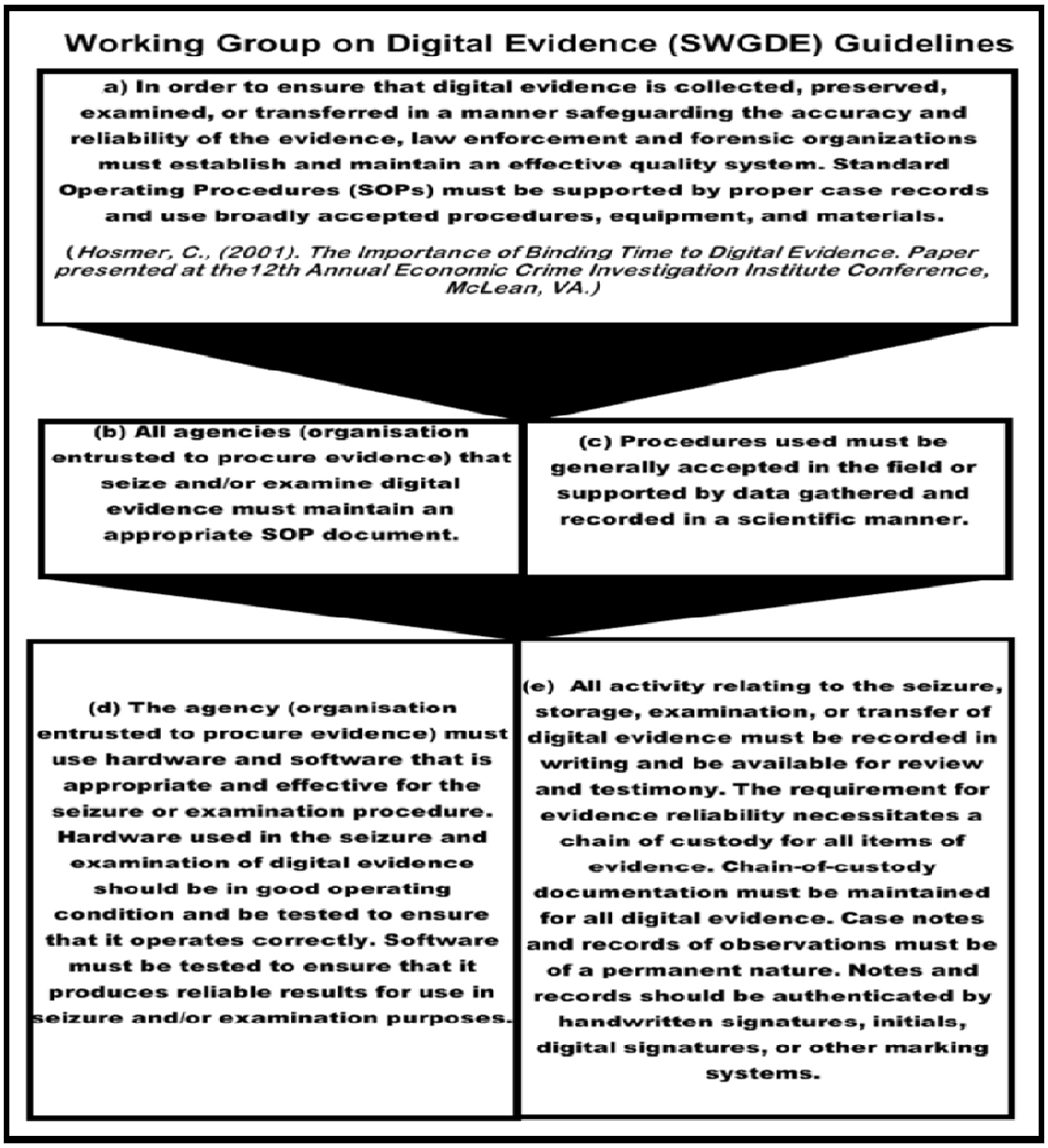

Diagram 3: Scientific Working Group on Digital Evidence (SWGDE) Guidelines

Further Scientific Working Group on Digital Evidence (SWGDE) prescribes that any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.[lxi]

Authentication and the best Evidence rule in the light of Evidence act-1872: is Printout from Computer Equivalent to its Digital Origin?

It is not an exaggeration to say that the most central problem in the whole of the law relating to computers, and perhaps more widely in the whole of contemporary law, is concerned with adaptation of the legal process to deal efficiently with the introduction of modern technology.

-Tapper, "Evanescent Evidence", (1993) 1(1) International Journal of Law and Information Technology, page: 35.

Computer output commonly takes the form of a printed document that may be:

(a) a direct replication of input data; or
(b) the results of the computer's processing that data according to a program; or
(c) the results of data processing by more than one computing, mechanical or other device acting in conjunction. [lxii]

And input data may be:

(a) collected by the computer itself whether on its own or in conjunction with other devices; or ;
(b) entered into the computer by human means; or
(c) a combination of (a) and (b). [lxiii]

Therefore, if a party wishes to rely on the contents of a printout document, the original computer output (data or file) must be produced. This means only the reduction of electronic information to paper (printout) may not be acceptable. It has been noted above that the routine visual and print manifestations of electronic or digital documents such as word-processing and e-mail lack vital metadata, the information about the author, date of creation, and history of distribution and editing. To produce these electronic documents in the court, the disclosing party must make them available in electronic form, preferably on media as close to the original as possible.[lxiv] They must then have the ability to copy the data in a manner that preserves the original electronic files to the greatest extent possible while protecting them from further mutation.[lxv] Generally, according to section 64 of the Evidence Act 1872, the authenticity of a document must be proven by the presence of primary evidence. This is called the Best Evidence Rule. In Omychund v Barker (1744)[lxvi], the best evidence rule was described as 'the best that the nature of the case will permit'. This commonly means that the party should produce the original documents. The Best Evidence Rule generally excludes oral evidence where documentary evidence exists. Printout of a file from a computer may fall within the ambit of this Section 64. There are a number of exceptions to the Best Evidence Rule prescribed in section 65 which may allow the printout admissible in absence

of its digital origin. Section 65 specifies seven cases in which secondary evidence of a document is admissible[lxvii], namely:

(1) when a document is in the possession of an opponent or of a person who is out of reach, or a person who fails to produce it after due process;

(2) when the existence ,condition or contents of the original are admitted in writing by person against whom it is proved;

(3) when the original cannot be found;

(4) when its production is physically impossible or highly inconvenient;

(5) where the document is of a public nature;

(6) where the original is one of which a certified copy is permitted by this Act;

(7) when the original consists of numerous accounts or other documents which cannot be conveniently examined in the court. [lxviii]

These rules focus upon reliability. As Evidence Act was enacted in 1872; these rules were developed before the advent of the computer. Therefore, reliability to an optimum level is ensured in the Act by calling for the source document and, where for good reason that is not available, demanding that a copy is demonstrated as far as possible to be a true copy as real evidence is evidence which the court can actually see, hear or touch in the form of an exhibit which can be analysed either by the court or by expert witnesses.[lxix] This will normally be by oral evidence from someone in a position to compare original with copy. Furthermore, the law of evidence has traditionally made distinctions between "primary" and "secondary" evidences. Primary evidence is "the best evidence, or that kind of proof which, under any possible circumstances, affords the greatest certainty of the fact in question . . ."[lxx] whereas secondary evidence "is all evidence falling short of this . . .".[lxxi] The law has, therefore, tended to restrict the admissibility of secondary evidence, particularly when primary evidence is available. Thus an original document has been considered better evidence than a copy. Therefore, a printout from a computer may be admissible in court if its digital origin is available. If the original computer derived data is unavailable, then printout may be admissible within the ambit of Section 65. It is contended that printouts are "copies" of "original" data entries on the hard drive of a computer leading to the conclusion that printouts may be admitted as copies because the originals cannot, for practical purposes, be produced. This view is supported by the following case:

In R v Nowaz [1976][lxxii], it was decided that even if the document is not readily available, secondary evidence of its contents cannot be adduced unless the case falls within the exceptions identified in the textbooks, one of which is that the original document cannot be found after "due search" [lxxiii]. In that case an issue arose whether the prosecution could adduce secondary evidence of the contents of a passport application in circumstances where the person holding the original application refused to produce it and could not be compelled to do so. James LJ, delivering the judgment of the court, referred to the dearth of authority on that issue in criminal cases, and continued (at p.832D):

"There are cases, which we have not found it necessary to consider in detail, which involved the civil law and evidence admissible in civil proceedings which clearly show that in circumstances

such as these where a document is not produced because it cannot be produced – because the person in whose custody it is cannot be compelled to produce it – then the secondary evidence is admissible."

He further said: "A general statement of the law can best be summarised, we think, in a passage to which our attention was invited in Professor Cross' book on Evidence, 4th ed. (1974), p.524), under the heading "Stranger's lawful refusal to produce document", which reads: When the original of a document is in the possession of a stranger to the litigation, the proper course for the party desiring to prove the contents of the document is to serve the stranger with a subpoena duces tecum. The stranger may, however, be able to establish a claim to privilege in respect of the document when secondary evidence of its contents becomes admissible.

Relating that to criminal proceedings, the subpoena duces tecum referred to is the equivalent of a witness summons requiring the attendance of a witness and production by the witness of the documents. That was complied with in this case we are told. The passage goes on: The governing principle is the same as that which covers the next two exceptions .... I interpolate, those are the exceptions of a lost document and production of the original document being impossible. Returning to the text: "... it is impossible to compel production of the document, and it will apply in cases in which the person in possession of the original is beyond the jurisdiction of the court; ..."

Vinelott J. considered the similar issue in Derby v. Weldon (No. 9)[lxxiv]. In the above case, the action was brought for breach of contract, misrepresentation, negligence, deceit, conspiracy to defraud and fraudulent breach of diduciary duty arising out of the trading activities of one of the plaintiffs while under the management of the first and second defendants. Certain of the defendants sought access to the computer database of the trading company (one of the plaintiffs), which formed part of the business records.

It was alleged that discovery was incomplete. The defendants contended that they were entitled to have access to the plaintiff's computer. What was initially offered by the plaintiff was an electronic copy of the relevant on-line database on disk and later the provision of copies or printouts of the information stored on the computer.

The following disputes arose:

(a) A new computer had been installed at the plaintiff. The defendants wished to satisfy themselves whether any part of the database of the computer then in use had been transferred to the database of the new computer, and if it had, whether it was capable of being recovered.
(b) It was suspected that certain accounts might still be missing. The defendants sought to ascertain whether any of the missing information could be retrieved from the history files.
(c) It was agreed that information recorded in the history files which is capable of being retrieved without extensive reprogramming was limited, but the history files included other material which could be retrieved by reprogramming the computer. The defendants wished to ascertain what information was capable of being retrieved by reprogramming.
(d) Transactions with unrelated parties were numerous and the computer printouts in that regard would occupy at least 75 large ring-binder files. It would facilitate the defendants' task of searching if they could have direct access to the database.

(e) The task of checking the results and answering queries that arose from their research would be eased through access to the database. Under arrangements made before the application, documents, in particular printouts had to be called for and there were often delays in finding the relevant document amongst the four to five thousand files that had been disclosed.

The court finds that a tape or disc on which material fed into a simple word processor is stored is a "document". Vinelott J. held that the database of a computer, in so far as it contained information capable of being retrieved and converted into readable form and whether stored in the computer or record in backup file, is a document for the purposes of the High Court rules governing discovery of documents. It was held that where there is no original document, a data message or a computer printout could be considered as the best available evidence. This decision could have consequences for the introduction of electronic originals.
An akin approach was observed in Barclays Western Bank v Creser, (1982)[lxxv]. The bank applied for default judgment and had to hand in the original agreement as evidence of its transaction with the defendant. The bank handed in an affidavit by one of its employees to the Magistrate, stating that it could not produce the original agreement between itself and the defendant because it had, due to lack of office space, embarked on a process of systematically recording its documentation by microfilm process and destroying the originals thereafter. The Magistrate declined to accept the microfilm evidence.

On appeal the court held that: "The best evidence rule is that no evidence is ordinarily admissible to prove the contents of a document except the original document itself. The exception to the rule is that on proof, inter alia, of the destruction of the document the contents of the document may be proved by secondary evidence. The only significance of the fact is, if it is a fact, that the party concerned deliberately destroyed a document, and, if it appears that that was done in contemplation of legal proceedings, possibly with a fraudulent objective that the court may decline to dispense with the requirement of production of the original. There was no question of anything of that sort in the present case. Litigation was not contemplated when the original was destroyed. And the destruction was done in the ordinary course of business."
But many do not agree with this argument; they promote the view that Evidence Act 1872 does not provide any option for covering computer derived evidence. It only deals with real world document which is "original" and digital documents along with its printout are not covered by the Act. Because, computer printout does not have an "original" in the sense, in which that term is generally understood in Evidence Act 1872. If there was an "original", it is likely to be regarded as the binary digits encoded into the computer. Therefore, it is not covered by Evidence Act 1872. Supporters of this concept often forward this argument that in Evidence Act 1872, the definition of evidence includes only two types of evidence, such as

i. oral
ii. documentary.[lxxvi]

Therefore, digital record or electronic records do not fall within the ambit of section-3. They further raise the argument based on the fact that the following sections of Evidence Act 1872

which deals with every aspect of admissibility of evidence, do not cover computer derived evidence.

Section	Provisions
Section 17 of Evidence Act 1872	An admission is a statement, ***oral or documentary***, which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned.
Section 32 (2)of Evidence Act 1872	Statements, written or verbal, of relevant facts made by a person who is dead, or who cannot be found, or who has become incapable of giving evidence, or whose attendance cannot be procured without an amount of delay or expense which under the circumstances of delay or expense which under the circumstances of the case appears to the Court unreasonable, are themselves relevant facts in the following cases : (1)……. (2) Or is made in course of business; When the statement was made by such person in the ordinary course of business, and in particular when it consists 'of any entry or memorandum made by him in books kept, in the ordinary course of business, or in the discharge of professional duty; or of an acknowledgement written or singed by him of the receipt of money, goods, securities or property of any kind, or of a document used in commerce written or signed by him; or of the date of a letter or other document usually dated, written or signed by him.
Section 34 of Evidence Act 1872	Entries in books of an account when relevant: Entries in books of account regularly kept in the course of business are relevant whenever they refer to a matter into which the Court has to inquire, but such statements shall not alone be sufficient evidence to charge any person with liability.
Section 35 of Evidence Act 1872	Relevancy of entry in public record made in performance of duty: An entry in any public or other official book, register or record, stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in performance of a duty specially enjoined by the law of the country in which such book, register or record is kept is itself a relevant fact.
Section 39 of Evidence Act 1872	What evidence to be given when statement forms part of a conversation document book or series of letters or papers: When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated government, or is contained in a document which forms part of a book, or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, book or series of letters or papers as the court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.
Section 59 of Evidence Act 1872	Proof of facts by oral evidence: All facts, except the contents of documents, may be provided by oral evidence.
Section 61 of Evidence Act 1872	Proof of contents of documents: The contents of documents may be provided either by primary or by secondary evidence.

Cont. table

Section 62 of Evidence Act 1872	Primary Evidence: Primary evidence means the document itself produced for the inspection of the court.
Section 63 of Evidence Act 1872	Secondary evidence. Secondary evidence means and includes - (1) certified copies given under the provisions hereinafter contained; (2) copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies; (3) copies made from or compared with the original; (4) counterparts of documents as against the parties who did not execute them; (5) oral accounts of the contents of a document given by some person who has himself seen it. Illustrations (a) A photograph of an original is secondary evidence of its contents, though the two have not been compared, if it is proved that the thing photographed was the original. (b) A copy, compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter, if it is shown that the copy made by the copying machine was made from the original. (c) A copy transcribed from a copy, but afterwards compared with the original is secondary evidence; but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original. (d) Neither an oral account of a copy compared with the original, nor an oral account of a photograph or machine-copy of the original, is secondary evidence of the original.
Section 64 of Evidence Act 1872	Proof of documents by primary evidence: Documents must be proved by primary evidence except in the cases hereinafter mentioned.
Section 65 of Evidence Act 1872	Cases in which secondary evidence relating to documents may be given: Secondary evidence may be given of the existence, condition or contents of a document in the following cases : (a) when the original is shown or appears to be in the possession or power of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such parson does not produce it ; (b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest; (c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time; (d) when the original is of such a nature as not to be easily moveable; (e) when the original is a public document within the meaning of section 74; (f) when the original is a document of which a certified copy is permitted by this Act, or by any other law in force in Bangladesh to be given in evidence;

	(g) when the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court, and the fact to be proved is the general result of the whole collection. In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible. In case (b), the written admission is admissible. In case (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible. In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents.
Section 67 of Evidence Act 1872	Proof of signature and handwriting of person alleged to have signed or written document produced: If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.
Section 68 of Evidence Act 1872	Proof of execution of document required by law to be attested: If a document is required by law to be attested, it shall not be used as evidence until one attesting witness at least has been called for the purpose of proving its execution, if there be an attesting witness alive, and subject to the process of the Court and capable of giving evidence: Provided that it shall not be necessary to call an attesting witness in proof of the execution of any document, not being a will which has been registered in accordance with the provisions of the Registration Act, 1908, unless its execution by the person by whom it purports to have been executed is specifically denied.
Section 69 of Evidence Act 1872	Proof where no attesting witness found: If no such attesting witness can be found, or if the document purports to have been executed in the Untied Kingdom, it must be proved that the attestation of one attesting witness at least is in his handwriting, and that the signature of the person executing the document is in the handwriting of that person.
Section 70 of Evidence Act 1872	Admission of execution by party to attested document: The admission of a party to an attested document of its execution by himself shall be sufficient proof of its execution as against him, though, it be a document required by law to be attested.
Section 39(18) of the General Clauses Act-1 897	Document is to include any matter written, expressed or described upon any substance by means of letters, figures of marks, or by more than one of those means, which intended to be used, or which may be used, for the purpose of recording that matter.

Fortunately the above arguments are to some extant useless due to the enactment of the Information & Communication Technology Act-2006. Under section 6 of ICT Act 2006, it was mentioned that "where any law provides that information or any other matter shall be in writing

or in the typewritten or printed form, then notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form, provided that information or any matter shall be accessible so as to be usable for subsequent reference." This provision indicates that digital documents or electronic documents will fall within the definition of 'document' and they hold the same status as any real world document.

As I said earlier that many put forward the argument that printouts are "copies" of "original" data entries on the hard drive of a computer, as a result printouts may be admitted as copies because the originals cannot, for practical purposes, be produced. The problem with this analogy is that it fails to recognise the transitory nature of the "original". An electronic original can be altered without leaving a trace[lxxvii] whereas alterations in a paper document are perceptible. So it is incorrect to say that a printout is always a copy of what is on the hard drive. The fact that depending on the timing of the print order, different paper documents may have been printed from the same file[lxxviii], is usually of forensic importance. That reality may be "obscured if one ignores the distinction between paper and electronic media. The Best Evidence Rule was developed when it was possible by human means to compare original with copy. The essential difference between paper and electronic media is that it is not possible by human agency to compare the "original" on the hard drive with the "copy" produced by printer or monitor."[lxxix] Therefore, printout cannot be admitted as secondary evidence. The aforementioned analogy is entirely inappropriate. A computer is used in the same way as a photocopying machine.[lxxx] Here the document is fed into a peripheral device known as a scanner. [lxxxi]This creates "an image of the document that is then stored by the computer in an image file. When the contents of the image file are sent by the computer to a printing device or a visual display, then it is, of course, possible to compare the source document with its copy."[lxxxii] If the original scanned document is not available, there is no reason why the electronic copy should not be admitted under an exception to the Best Evidence Rule subject to human verification where possible, that the copy accords with the original. [lxxxiii] Bangladeshi courts have allowed videocassettes, tape recordings and snapshot of hand cameras as admissible evidence. Tape recordings received the same footing as photographs and documents under section 3 of the Evidence Acts. A videocassette is a document within the meaning of the Evidence Act and is accordingly admissible in the court as per Mrs. Khaleda Akter v. the State.[lxxxiv] On the basis of the decisions of the cases like Khaleda Akter v. State[lxxxv], M. P. Verma v. Surinder Kaur[lxxxvi] and Z. B. Bhukhari v. B. R. Mehra[lxxxvii], it is my view that an electronic or computer derived record would fall within the definition of document. Further, in the light of the following persuasive precedence, it can be presumed that computer generated evidence may be admitted as primary evidence. For example, film strips of radar images[lxxxviii]and Partlow Charts (used for recording the temperature in a refrigerated container)[lxxxix] earned admissibility as primary evidence. Provided a proper evidential foundation is laid to show that electronically generated charts or analyses relate to the item in question, then that information may be admissible as primary evidence.[xc] Furthermore, in Longcroft-Neal v Police [1986][xci], videotape was held to be a document for the purposes of s 2 of the now repealed Indecent Publications Act 1963. In Snow v Hawthorn [1969] [xcii],tape recording was held to be a document; and in NZI Insurance NZ Ltd v Hinton, Hill and Powles [1996] [xciii],the court admitted

the documents copied from a computer on to compact discs. In the light of the above discussion, it may be concluded that Information & communication Technology Act -2006 and the purposive interpretation of the provisions of Evidence Act-1872 allow digital data as primary evidence to be admissible in the court. A printout from a computer receives the status of secondary evidence in the presence of its digital origin which is functional equivalent of a real world document. On the other hand, nonexistence of digital origin of a printout makes it admissible if it falls within the threshold of section 65 of Evidence Act 1872.
But many promote the view that "a workable approach may be to regard both the data stored in electronic form on the computer and the printout as primary evidence. Both are products of computing devices and, provided there is sufficient evidence of the correct working of those devices,"[xciv] the law should allow the printout to pass the threshold of admissibility.[xcv] Its reliability as a replication of, or derivation from, source data, then becomes a matter of weight.[xcvi]
But difficulties have arisen in the application of the primary and secondary evidence rules to computer generated evidence in this regard. For example, what will be the status of a printout if its original is accessible? In the presence of primary evidence, secondary evidence does not carry sufficient weight. Therefore, a printout will never be equivalent of its digital origin.

Despite of the fact that I have already discussed various issues of digital evidence, the question – 'whether a printed document is to be considered as equivalent of the original document or the actual file saved on computer' still remains unanswered. This question may be answered if we look into the English case Kajala v Noble (1982) [xcvii].

In Kajala v. Noble, [xcviii] Kajala was convicted of breach of the peace and threatening behaviour after being identified from a videotape copy of original BBC news footage. It was argued on his behalf before the Court of Criminal Appeal that the video was inadmissible because original film lodged in the archives of the BBC ought to have been produced. In short there had been a breach of the Best Evidence Rule.
Ackner L.J., delivering the judgment of the Court, said: "The old rule, that a party must produce the best evidence that the nature of the case will allow, and that any less good evidence is to be excluded, has gone by the board long ago. The only remaining instance of it is that, if an original document is available in one's hands, one must produce it; that one cannot give secondary evidence by producing a copy. Nowadays we do not confine ourselves to the best evidence. We admit all relevant evidence. The goodness and badness of it goes only to weight, and not to admissibility: Garton v. Hunter [1969] 1 All E.R. 451, per Lord Denning M.R. at 453e; see also Archbold, Criminal Pleading, Evidence and Practice (40th ed.), para. 1- 001. In our judgment, the old rule is limited and confined to written documents in the strict sense of the term, and has no relevance to tapes or films."
In Kajala v. Noble[xcix] ,the court allowed a copy of a video tape to be introduced in evidence while the original remained with the BBC. The court in this instance was less concerned with the initial hurdle of admissibility than with the actual probity of the evidence.

The above decision was based on the comments of Lord Denning in Garton v Hunter [1969][c]. In Garton v Hunter [1969][ci], Lord Denning stated: "That old rule has gone by the board long ago

..... nowadays we do not confine ourselves to the best evidence." And in Masquerade Music Ltd v Springsteen [2001][cii], referring to the rule, Jonathan Parker LJ stated: "..... the time has now come when it can be said with confidence that the best evidence rule, long on its deathbed, has finally expired."

It is true that Kajala v Noble (1982) [ciii] takes a pragmatic view of new technology. The priority is "to prevent rules of evidence developed with older technology in mind from obscuring the probative value of more modern means of communication and storage media."[civ] If one remembers that the general purpose of the Best Evidence Rule is to preserve the quality of evidence, the admission of computer records does not threaten that aim provided their greater potential for corruption is guarded against.[cv] Here the emphasis ought to be upon authentication, that is, the steps taken to satisfy the court that what is proffered is what it purports or is claimed to be. The steps required to authenticate computer evidence must depend on the extent to which the technology is "tried and tested" (the reliability of the output in terms of the system's design) and, in most cases must take into account the transient [cvi] nature of electronic records. [cvii]
In the light of this well recognised case, it can be concluded that printout cannot be equivalent of an original data from which it was generated. But the original data source not always required for ensuring the authenticity of the printout, a genuine copy of the original data source may be admitted as primary evidence to validate authenticity of the printed document.

Concluding Remarks: There is a perception, mostly unjustified, that computer generated evidence or digital evidence somehow changes the true nature of the original evidence and is therefore untrustworthy. If presented properly with due authentication, digital evidence can be capable of offering tremendous help to the courts. In many cases, digital evidence has allowed the courts to gain valuable information which to some extant ensure correct verdict. Further, it has allowed the court to receive evidence that it would not have been able to receive without the assistance of digital technology. But unfortunately, in our country, courts are not fortunate enough to be aided by digital technology as the existing legal framework is not equipped to handle digital evidence. The laws relating to the admissibility of documentary evidence in Bangladesh are convoluted and not designed to deal with electronic data in mind. In the absence of any amendment, Evidence Act (I of 1872) is not modern enough to facilitate the concept of digital evidence. It is surprising to know that we don't have any statutory provision to deal with any digital evidence except the ICT Act. India and Bangladesh both inherited the old British colonial regulation from their inception, but India managed to amend its statutes and became very much familiar with the impact of modern high-tech gadgets. The Indian Evidence Act (I of 1872) as amended by the Information Technology Act 2000 elaborately deals with the issues of admissibility of electronic records (Section 65-B). But as a colonial cousin we failed to do the same. We are to some extent living in the realm of law, having the characteristics of a pre-modern society. We have successfully enacted ICT Act in 2006 which attempts to render the admissibility of digital evidence, including electronic evidence, but we were unable to eliminate foreseeable lacunas in it. As a result the ICT Act 2006 failed to acknowledge a range of forensic procedures and practices which are very much needed in ensuring authenticity of a data. Further, poor acquisition guideline made the process of retention of digital evidence so vulnerable that ensuring

authenticity of a data became an impracticable task. Therefore, an amendment of both the Act is a dire need. As the chances of success in litigation depend heavily on the availability of strong evidence, new or amended Evidence Act is essential for handling digital evidence. New or amended Evidence Act should suggest different procedures for authentication of electronic evidence, as with the establishment of a complete chain of custody, from the person who first copied the data to the person who produced the printout for the trial, or the use of electronic signatures. We know almost every technological change has created opportunities for new forms of crime, albeit often variants on existing ones , therefore, new strands of legislation and regulation should be imposed to deal with computer generated data and other technology related legal issues.

Works Cited (Excluding Footnotes)

1. *H. Smith(1996), The Future of Intellectual Property in an Online World, Computers and Law, Vol. 7 Issue 2, June/July 1996, pp. 33-37.*
2. *John A., Jr. Livingood (1994),Admissibility and reliability of expert scientific testimony after Daubert. (Daubert v. Merrell Dow Pharmaceuticals, Inc.),Defense Counsel Journal (Refereed) January 1, 1994 ,Volume: 61 Issue: n1 Page: 19-27 ,Publisher: International Association of Defense Counsels.*
3. *Mark Pollitt (Editor), Sujeet Shenoi (Editor)(2005) ,Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, ... in Information and Communication, Publisher: Springer; 1 edition (November 15, 2005) Technology)*
4. *Sidor, G. and S. Rogers. (2002), Electronic Evidence is Superior to Paper Evidence, The Lawyers Weekly. 21(44). March 29, 2002.pp.7-9.*
5. *Shear, K. R. (2003) ,Orders Freezing Backups-An Approach that Should Leave Courts Cold, Digital Discovery and e-Evidence, (3)7, July,2003, pp. 3-5.*
6. *Keena, J. R. (2002) ,E-Discovery: Unearthing Documents Byte by Byte, Bench & Bar of Minnesota, Mar. 2,2002,pp.11-31.*
7. *Arent, L. M., R. D. Brownstone, and W.A. Fenwick. (2002), E-Discovery: Preserving, Requesting and Producing Electronic Information, Santa Clara Computer and High Technology Law Journal. 19 (131) December, 2002.pp.56-87.*
8. *Brenner SW (2001) Cybercrime investigation and prosecution: the role of penal and procedural law. E-law: Murdoch University electronic journal of law 8(2). http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html*
9. *De Wilde F (2006) Courtroom technology in Australian courts: an exploration into its availability, use and acceptance. Qld lawyer 26: 303–328*
10. *Goodman MD & Brenner SW (2002), The emerging consensus on criminal conduct in cyberspace. UCLA journal of law and technology 3.http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php*
11. *Kennedy & Davids (1996), Bartleby the Cryptographer: Legal Profession Prepares for Digital Signatures, N.Y.L.J., Jan 22, 1996, at S4.*
12. *Achinstein, Peter (1983). "Concepts of Evidence", in Achinstein (ed.) The Concept of Evidence, Oxford: Oxford University Press.*
13. *Colin Tapper (2010)Cross & Tapper on Evidence, Oxford University Press 12th edn.*
14. *Conee, Earl and Feldman, Richard (2004). Evidentialism,Oxford: Oxford University Press.*

15. *Halim,Abdul(2008),The Law of Evidence:Theoty and Practice,CCB Foundation.*
16. *Feldman, Richard (2004). "Having Evidence" in David Austin (ed.) Philosophical Analysis, Dordrecht: Kluwer Academic Publishers, Reprinted by Conee and Feldman (2004).*
17. *Glymour, Clark (1980). Theory and Evidence, Princeton, NJ: Princeton University Press.*
18. *Horwich, Paul (1982). Probability and Evidence, Cambridge: Cambridge University Press.*
19. *Robert C. Newman (2007), Computer Forensics: Evidence Collection and Management, Publisher: Auerbach Publications .*
20. *Eoghan Casey BS MA (2004) ,Digital Evidence and Computer Crime, Second Edition Publisher: Academic Press; 2 edition (March 22, 2004)*
21. *Shira Scheindlin, Daniel J. Capra, (2008),Electronic Discovery and Digital Evidence: Cases and Materials (American Casebook) - Hardcover (Dec. 4, 2008), Publisher: West; 1 edition (December 4, 2008),*
22. *Karen A. Schuler ,Robert C. Newman (2008) ,E-discovery: Creating and Managing an Enterprise wide Program - A Technical Guide to Digital Investigation and Litigation Support , Publisher: Syngress; 1 edition (November 3, 2008)*

Endnotes

---

[i] *Nimsger, Kristin M. and Michele C.S. Lange. (2009) ,Computer Forensics Experts Play Crucial Role, The Lawyers Weekly. 22(2) May 10,2009,pp.27.*

[ii] *Zaslow, J. (2003), To Fight E-mail Sharing, Firms Try New Rules, Software, Wall Street Journal, May 28, 2003,pp.98.*

[iii] *Varchaver, N. (2003) ,The Perils of E-Mail,Fortune. Feb. 3, 2003.*

[iv] *Streza, R. (2003) Discovery Unplugged: Should Internal E-mails be Privileged Confidential Communications? Defense Counsel Journal, 70(1), January 1. pp. 36-41at 39.*

[v] *P. Sommer(1999), Clueless: Computer Forensics, Secure Computing, November 1995, pp. 15-21*

[vi] *http://www.wisegeek.com/what-is-computer-evidence.htm, retrieved on 1/12/2009.*

[vii] *Robert C. Newman (2007), Computer Forensics: Evidence Collection and Management, Publisher: Auerbach Publications ,pp.332*

[viii] *R. v. Shephard [1993] A.C. 380 and R. v. Cochrane [1993] Crim.L.R. 48. S.69*

[ix] *Michael J L Turne (2010)r, Computer Evidence, http://www.computerevidence.co.uk/, retrieved on 11/4/2010.*

[x] *http://www.swgde.org/*

[xi] *http://www.gladyshev.info/publications/thesis/chapter2.pdf*

[xii] *Ashraf Mozayani and Carla Noziglia (2007), Forensic Science and Medicine: The Forensic Laboratory Handbook Procedures and Practice, Humana Press, pp. 70-90 at 80.*

[xiii] *Eoghan Casey (2004) Digital evidence and computer crime: forensic science, computers and the Internet, Academic Press.*

[xiv] *http://books.google.com/books?id=Xo8GMt_AbQsC&pg=PA12&lpg=PA12&dq=definition+of+digital+evidence&source=bl&ots=-XV*

[xv] *C .Miller (1992),Electronic Evidence--Can You Prove the Transaction Took Place?, Computer Lawyer, Vol. 9 No. 5, pp. 21-33 at 27, May 1992*

[xvi] *C .Miller (1992),Electronic Evidence--Can You Prove the Transaction Took Place?, Computer Lawyer, Vol. 9 No. 5, pp. 21-33at 22, May 1992*

[xvii] *C. Miller, (1992), Electronic Evidence--Can You Prove the Transaction Took Place?, Computer Lawyer, Vol. 9 No. 5, pp. 21-33 at 33, May 1992.*

[xviii] *American Heritage Dictionary,http://education.yahoo.com/reference/dictionary/entry/authentic*

[xix] *Dictionary.com ,http://dictionary.reference.com/browse/authentic*

[xx] *American Heritage Dictionary : http://education.yahoo.com/reference/dictionary/entry/authentic*

[xxi] *B. Wright, The Law of Commerce (2nd ed., Little Brown, Boston, 1995), p. 7.1*

[xxii] *Reed, (1990-91) 2 C.L.S.R. 13-16*

[xxiii] *C. Waelde and L. Edwards(1996), Defamation and the Internet: a Case Study of Anomalies and Difficulties in the Information Age, International Review of Law, Computers and Technology, Vol. 10 No. 2, 1996, pp. 263-294.*

[xxiv] *Edward Imwinkelried(1991), The Debate in the DNA Cases Over the Foundation for the Admission of Scientific Evidence: The Importance of Human Error as a Cause of Forensic Misanalysis, 69 WASH. U. L. Q. 19 (1991).*

[xxv] *Fred Galves(2000), Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, 13 HARV. J. L. & TECH. 161, 229-30 (2000).*

[xxvi] *FED. R. EVID. 1001. Variations of this rule have been adopted by nearly every state in the United States.*

[xxvii] *Ohio v. Morris, 2005 Ohio 599, (Ohio Ct. App. Wayne County, Feb. 16, 2005).*

[xxviii] *509 U.S. 579 (1993)*

[xxix] *International Organization on Computer Evidence (IOCE) First Responders Guide Template (Dec. 14, 2000), available at: http://ncfs.org/documents/ioce2000/reports/firstResponders.pdf*

[xxx] *Holt v Auckland City Council [1980] 2 NZLR 124*

[xxxi] *The Federal Rules of Evidence (USA) s 803(6); Transport Indem- nity Co v Seib 132 NW 2d 871 (1965), 874–875; and State of New Mexico for the Use of Electric Supply Co Inc v Kitchens Construction Inc 750 P 2d 114 (NM 1988) 114, 117.*

[xxxii] *Marac Financial Services v Stewart [1993] 1 NZLR 86.*

[xxxiii] *Eoghan Casey BS MA (2004) ,Digital Evidence and Computer Crime, Second Edition Publisher: Academic Press; 2 edition (March 22, 2004),pp.211.*

[xxxiv] *Marac Financial Services Limited v Stewart [1993] 1 NZLR 86*

[xxxv] *Ministry of Agriculture and Fisheries v Thomas [1994] DCR 486*

[xxxvi] *Ministry of Agriculture and Fisheries v Thomas [1994] DCR 486, 505 citing from Holt v Auckland City Council [1980] 2 NZLR 124 (CA) 128. See also, the Western Australian case of Zappia v Webb [1974] WAR 15, 17 to which Judge RL Kerr also referred in Thomas.*

[xxxvii] *Ministry of Agriculture and Fisheries v Thomas [1994] DCR 486, 505*

[xxxviii] *Gringras gives some support to this view when referring to "programmed intention" in the context of the question whether a party who has pre-programmed a computer to enter into a contract in any given circumstance can have had the necessary intention to form a binding contract (1997 29; see also Nicoll 1998 48_49; Myburgh 1993 327; and paras 57_64 of this report).*

[xxxix] *UN 1996: Draft Guide to enactment of the Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication, UN Doc. A/CN.9/426 (Apr. 24, 1996)*

[xl] *UN 1995: Draft Guide to enactment of the Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication, (UN reference A/CN.9/WG.IV/WR.64 31 January 1995).*

[xli] *Noblett, M.G. (1995). Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. Proceedings of the 11th INTERPOL Forensic Science Symposium, Lyon, France. Boulder, CO: The Forensic Sciences Foundation Press.*

[xlii] *Livermore (1998) J et al, 'Electronic Bills of Lading and Functional Equivalence', 1998 (2) THE JOURNAL OF INFORMATION, LAW AND TECHNOLOGY (JILT).*

<http://elj.warwick.ac.uk/jilt/ecomm/98_2liv/>.

[xliii] *Mark Pollitt (Editor), Sujeet Shenoi (Editor)(2005) ,Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, ... in Information and Communication, Publisher: Springer; 1 edition (November 15, 2005) Technology)*

[xliv] *Scientific Working Group on Digital Evidence and International Organization on Digital Evidence. (2000). Digital Evidence: Standards and Principles [on-line]. Forensic Science Communications, 2(2). Available: http://www.fbi.gov/hq/lab/fsc/ backissu/april2000/swgde.htm*

[xlv] *Ahmed, Zulfiquar, A Text Book on Cyber Law in Bangladesh, NLBC, Pp. 78*

[xlvi] *Hosmer, C., Feldman, J., & Giordano, J., (1998). Advancing Crime Scene Computer Forensics Techniques. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.*

[xlvii] *Robert Simmons , J. Daniel Lounsbery (1994) ,Admissibility of computer-animated reenactments in federal courts. (Demonstrative Evidence): An article from: Trial Magazine,September 1, 1994,Publisher: Association of Trial Lawyers of America,Volume: 30 Issue: 09 Pp. 78.*

[xlviii] *159 A Crim R 416 [2006] NTSC 14 (21 February 2006).*

[xlix] *Bird v Peach [2006] NTCA 7 (28 August 2006).*

[l] *The data on computers, especially the data on network servers, will usually be duplicated onto digital storage media on a regular schedule for disaster-recovery purposes, thus creating another copy set of the document (including all pre-existing copies and versions). Ideally, the backup media will be retained for only a few days or a month, and then be destroyed or recycled as is made redundant by subsequent backups. Unfortunately, the legal, popular, and even technical press report that these backups are usually saved. Often the data on the backups (and sometimes the backups themselves) are treated as archival. The data are transferred to more permanent digital or optical media, usually without any selectivity or reference to conventional records-retention policies.*

[li] *Streza, R. (2003),Discovery Unplugged: Should Internal E-mails be Privileged Confidential Communications?, Defense Counsel Journal, 70(1), January 1, 2003. pp. 36-41.*

[lii] *Kabushiki Kaisha Sony Computer Entertainment v Stevens [2002] FCA 906 (26 July 2002)*

[liii] *Digicel (St Lucia) Ltd. & Others v. Cable & Wireless Plc & Others (2008) E.W.H.C. 2522*

[liv] *Qualitative analysis: A Guide to Best Practice, ISBN 0 85404 462 0, Royal Society of Chemistry, Cambridge, 1998.*

[lv] *Standard Practice for Receiving, Documenting, Storing and Retrieving Evidence in a Forensic Science Laboratory, ASTM E 1459-92*

[lvi] *Robert Simmons , J. Daniel Lounsbery (1994) ,Admissibility of computer-animated reenactments in federal courts. (Demonstrative Evidence): An article from: Trial Magazine, September 1, 1994,Publisher: Association of Trial Lawyers of America,Volume: 30 Issue: 9 Pp. 79.*

[lvii] *Streza, R. (2003),Discovery Unplugged: Should Internal E-mails be Privileged Confidential Communications?, Defense Counsel Journal, 70(1), January 1, 2003. pp. 36-41.*

[lviii] *Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.*

[lix] *Schneier, B. (1996.) Applied Cryptography (2nd ed.), John Wiley & Sons.*

[lx] *Hosmer, C., (2001). The Importance of Binding Time to Digital Evidence. Paper presented at the12th Annual Economic Crime Investigation Institute Conference, McLean, VA.*

[lxi] *Carrie Morgan Whitcomb (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1.*

[lxii] *Hosmer, C., (2001). The Importance of Binding Time to Digital Evidence. Paper presented at the12th Annual Economic Crime Investigation Institute Conference, McLean, VA.*

[lxiii] *Carrie Morgan Whitcomb (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1.*

[lxiv] *Hosmer, C., (2001). The Importance of Binding Time to Digital Evidence. Paper presented at the12th Annual Economic Crime Investigation Institute Conference, McLean, VA.*

[lxv] *Carrie Morgan Whitcomb (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1.*

[lxvi] *Omychund v Barker (1744) 1 Atk. 21 at p. 49, per Lord Hardwicke.*

[lxvii] *Justice Idris Ali in Husan Ali v Azmaluddin (14 DLR 392) described these rule in simple language, which are stated here.*

[lxviii] *A copy of an inscription on a tombstone, for example.*

[lxix] *Carrie Morgan Whitcomb (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1.*

[lxx] *Sidor, G. and S. Rogers. (2002) "Electronic Evidence is Superior to Paper Evidence," The Lawyers Weekly. 21(44). March 29.*

[lxxi] *Greenleaf (1972) and Thayer (1898) ,Documentary Evidence and Judicial Notice, para 152 citing, http://www.lawcom.govt.nz/UploadFiles/Publications/Publication_49_95_R50/html/Publication_49_95_R50_93.html?gInitialPosX=10px&gInitialPosY=10px&gZoomValue=100*

[lxxii] *R v Nowaz [1976] 1 WLR 830 CA*

[lxxiii] *Colin Tapper (2010),Cross & Tapper on Evidence, Oxford University Press 12th edn. p.755*

[lxxiv] *Derby v. Weldon (No. 9) [1991] 2 All E.R. 901. This case is commented upon by Tapper, "Evanescent Evidence", (1993) 1 International Journal of Law and Information Technology 35, 42.*

[lxxv] *Barclays Western Bank v Creser, 1982 (2) SA 104 (T),*

[lxxvi] *Section 3 of Evidence Act 1872*

[lxxvii] *Except where appropriate encryption techniques have been used.*

[lxxviii] *In the sense that its name remains the same.*

[lxxix] *PT-001-A1 June 1998 Guidance on the Conduct of Proficiency Tests and Collaborative Exercises within ENFSI, European Network of Forensic Science Institutes Yearbook, 1998-1999*

[lxxx] *Withers, K. J. (2000) "Killing the Vampire: Computer Users, Facing Discovery, Attempt to Make the 'Delete' Key Stick. Part I." Federal Discovery News. Feb. 15.*

[lxxxi] *Sidor, G. and S. Rogers. (2002) "Electronic Evidence is Superior to Paper Evidence," The Lawyers Weekly. 21(44). March 29.*

[lxxxii] *Withers, K. J. (2000) "Killing the Vampire: Computer Users, Facing Discovery, Attempt to Make the 'Delete' Key Stick. Part I." Federal Discovery News. Feb. 15.*

[lxxxiii] *Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.*

[lxxxiv] *Mrs. Khaleda Akter v. the State ,37 DLR 275*

[lxxxv] *Mrs. Khaleda Akter v. the State ,37 DLR 275*

[lxxxvi] *M. P. Verma v. Surinder Kaur(1982), AIR1982 SC 1043*

[lxxxvii] *Z. B. Bhukhari v. B. R. Mehra (1975),AIR 1975 SC 1788.*

[lxxxviii] *The Statue of Liberty [1968] 2 All ER 195, 196*

[lxxxix] *OEM International Limited v The Ship "Wellington Maru" (1997) 11 PRNZ 142*

[xc] *OEM International Limited v The Ship "Wellington Maru" (1997) 11 PRNZ 142*

[xci] *Longcroft-Neal v Police [1986] 1 NZLR 394 (CA),*

[xcii] *Snow v Hawthorn [1969] NZLR 776, 777*

[xciii] *NZI Insurance NZ Ltd v Hinton, Hill and Powles [1996] 1 NZLR 203, 209*

[xciv] *Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.*

[xcv] *Subject to hearsay or other objections.*

[xcvi] *Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.*

[xcvii] *(1982) 75 Cr.App.R. 149.*

[xcviii] *(1982) 75 Cr.App.R. 149.*

[xcix] *(1982) 75 Cr.App.R. 149. Note that the apparently inconsistent decision of Kilner Brown J. in R. v. Stevenson [1971] 1 All E.R. 678 was decided more on the basis that proffered tape recordings may have been tampered with. It is unlikely that properly authenticated true copies would have been rejected on the basis of the Best Evidence Rule.*

[c] *Garton v Hunter [1969] 2 QB 37 at 44*

[ci] *Garton v Hunter [1969] 2 QB 37 at 44*

[cii] *Masquerade Music Ltd v Springsteen [2001] EWCA Civ 563*

[ciii] *Kajala v Noble (1982) 75 Cr App R 149 at 152*

[civ] *Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.*

[cv] *Hosmer, C., Feldman, J., & Giordano, J., (1998). Advancing Crime Scene Computer Forensics Techniques. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.*

[cvi] *It should be remembered, however, that computer records can be rendered "tamper proof". For example, by using special media and by adopting encryption techniques.*

[cvii] *Marac v. Stewart [1993] 1 N.Z.L.R. 86 at 92.*